KOREAN PATENT ABSTRACTS(KR)

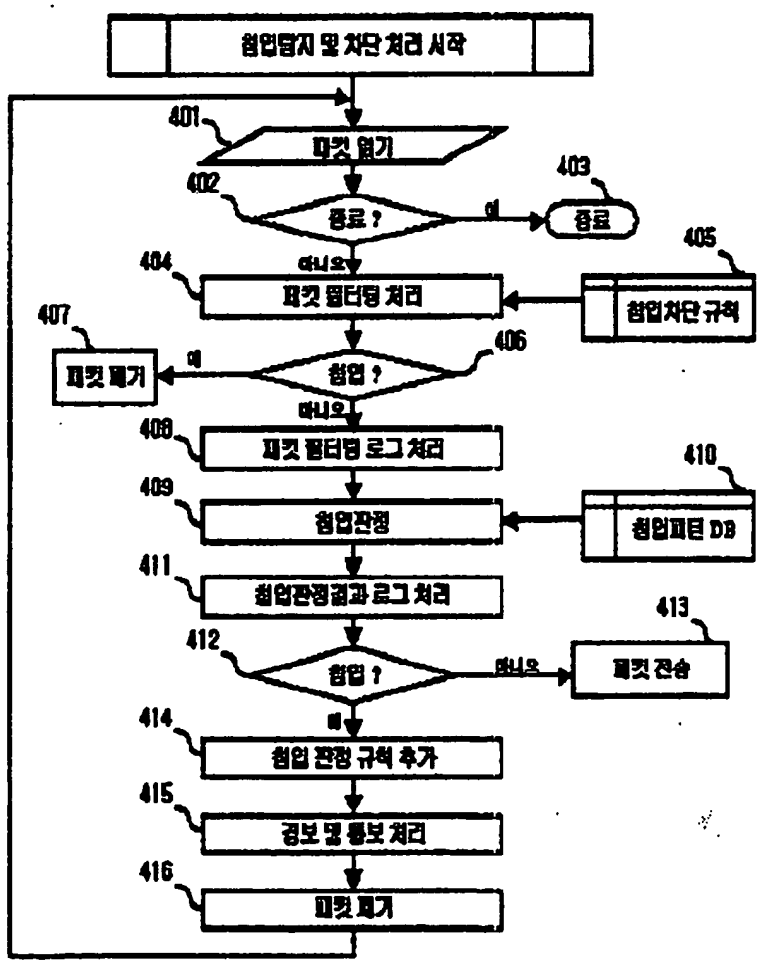
Document Code: A
(11) Publication No. 1020000072707 (43) Publication.Date. 20001205
(21) Application No. 1020000055323 (22) Application Date. 20000920
(51) IPC Code:
H04L 12/22

(71) Applicant:
SECUVE
(72) Inventor:
EUN, YU JIN
HONG, GI WAN
HONG, GI YUNG
KIM, JAE MYEONG
LEE, MIN GU

(30) Priority:

(54) Title of Invention
METHOD FOR AUTOMATICALLY MONITORING INVASION AND CUTTING OFF HACKING IN REAL TIME

Representative drawing



(57) Abstract:

PURPOSE: A method for automatically monitoring invasion and cutting off hacking in real time, is provided to pass hardware and software simultaneously performing the functions of invasion cutoff and monitoring for every packet information accessing to an internal network through an external information and communication network, so as to completely cut off related packet and messages.

CONSTITUTION: A data packet accessed through an external information and communication network like the Internet is read from a packet collector. If the data packet is for completion, the steps are ended. If the data packet is not completed, packet filtering is processed for packet information which is a result of the packet reading, by referring to an invasion cutoff rule in an invasion cutoff rule storage. If the data are for invasion, the packet is perished. If the data are not for invasion, a log processor performs packet filtering log processing. Invasion monitoring engine decides invasion by referring

to an invasion pattern within invasion pattern database storage. Log processing of a result of invasion decision is performed to the log processor. If a decided result is not for invasion, packet transmission is performed. If the decided result is for invasion, the invasion monitoring engine performs an invasion cutoff rule automatically adding packet information to an invasion cutoff rule storage. Alarm and notification are performed to an alarm and notification processor. The packet is perished and the first step is returned.

if display of image is failed, press (F5)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.
H04L 12/22(조기공개)

(11) 공개번호 특2000-0072707
(43) 공개일자 2000년12월05일

(21) 출원번호 10-2000-0055323
(22) 출원일자 2000년09월20일

(71) 출원인 주식회사 시큐브, 홍기용
대한민국
463-500
경기도 성남시 분당구 구미동 18번지 시그마투 D-217

(72) 발명자 홍기용
대한민국
463-500
경기도 성남시 분당구 구미동 221번지 무지개마을 505-104

은유진
대한민국
440-200
경기도 수원시 장안구 조원동 881번지 한일타운아파트 104-1801

홍기완
대한민국
135-081
서울특별시강남구역상1동745-10102호

이민구
대한민국
449-910
경기도 용인시 구성면 상하리 447 풍림아파트 106-403

김재영
대한민국
143-130
서울특별시 광진구 화양동 9-5

(77) 심사청구 있음

(54) 출원명 실시간 침입탐지 및 해킹 자동 차단 방법

요약

본 발명은 인터넷 등 정보통신망을 통하여 외부 네트워크에서 내부 네트워크로 접근하는 모든 데이터에 대하여 불법적인 침입을 실시간 탐지 및 차단하여 내부시스템의 안전·신뢰성을 확보할 수 있는 실시간 침입탐지 및 불법 해킹 자동 차단방법에 관한 것이다.

이를 위해 본 발명은 침입차단시스템의 패킷필터링 기능과 침입탐지시스템의 침입탐지엔진 기능을 상호 연동시켜, 침입탐지엔진이 침입을 탐지할 경우 침입과 관련된 패킷 및 메세지를 실시간 자동으로 완전 차단할 수 있는 기능을 제공한다.

대표도

도2

색인어

침입탐지, 침입차단, 패킷필터링, 침입판정, 침입패턴, 해킹방지

명세서

도면의 간단한 설명

제1도는 본 발명이 적용되는 인터넷 등 외부 정보통신망과 내부망 사이에서의 실시간 침입탐지와 연동하는 불법해킹 자동 차단 장치내의 침입탐지및차단처리부, 침입차단규칙설정·조회처리부, 침입패턴DB설정·조회처리부 등을 포함하는 구성도.

제2도는 본 발명이 적용되는 실시간 침입탐지와 연동하는 불법해킹 자동차단 장치에서의 네트워크접속처리부, 패킷수집부, 패킷필터링처리부, 침입탐지엔진, 침입차단규칙저장부, 침입패턴DB저장부, 침입차단규칙설정·조회부, 침입패턴DB설정·조회부, 관리자콘솔, 로그처리부, 경보및통보처리부 등의 상호 동작도.

제3도는 본 발명의 전체흐름 개략도.

제4도는 본 발명의 침입탐지및차단처리부 흐름도.

제5도는 본 발명의 침입차단규칙설정조회부 [redacted]도.

제6도는 본 발명의 침입패턴DB설정조회부 흐[redacted]

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 외부 정보통신망을 통하여 내부망으로 접근하는 모든 패킷 정보를 수집하여 불법적으로 침입하려는 시도를 탐지하여 비정상 행위 패킷을 사전에 차단하는 것으로, 특히 서비스거부공격(DOS, Denial Of Service)을 원천적으로 방지하여 정상 행위 데이터의 흐름을 안전하게 하며 공격자로 부터 내부 시스템을 보호하기 위한 실시간 침입탐지 및 침입차단 방법에 관한 것이다.

이와 관련한 종래의 기술은 외부 네트워크상에 존재하는 호스트들의 허가되지 않은 접근으로 부터 내부 네트워크상에 존재하는 시스템들을 보호하기 위해 특정 서비스 및 네트워크 주소에 관련된 네트워크 접속만을 허용하는 방법으로 보안기능을 제공하고 있으나, 서비스거부공격과 같은 공격에 취약할 수 밖에 없는 제한적인 기능만을 제공하였다. 이의 보안을 위해 네트워크상의 패킷 정보를 수집하여 침입패턴DB를 참조하여 불법적인 침입 행위를 탐지하여 관리자에게 통지하는 침입탐지시스템이 등장하였으나 관리자가 직접 개입하여 처리하여야 하는 문제점으로 인하여 침입행위에 대한 적절히 대응하지 못하는 문제점을 가지고 있다.

이와 같이 침입차단시스템 및 침입탐지시스템의 독립적인 작동은 웹서버 등에 대한 서비스거부공격과 같은 다양한 공격방법으로 인한 특정 시스템 및 네트 워크 보안에 대해 실시간으로 적절히 대응하지 못함으로써 공격자로 부터의 특정 네트워크 서비스를 마비시키는 부하 위협에 무방비 상태로 노출되어 있는 상태이다.

발명이 이루고자 하는 기술적 과제

따라서 본 발명은 상기와 같은 문제점을 해결하기 위해 외부 정보통신망을 통하여 내부 네트워크로 접근하는 모든 패킷 정보에 대해 침입차단 기능과 침입 탐지 기능을 동시에 수행하는 H/W 또는 S/W를 통과하게 하여 침입행위와 관련된 패킷 및 메세지를 원천적으로 차단함으로써 내부 시스템을 안전·신뢰성 있게 운영할 수 있도록 하는데 그 목적이 있다.

이와 같은 목적을 달성하기 위하여 본 발명은 침입차단시스템의 패킷필터링처리 기능과 침입탐지시스템의 침입탐지엔진 기능을 상호연동시킴으로써, 침입탐지엔진이 침입을 탐지할 경우 실시간 자동으로 침입차단규칙에 이를 추가하여 패킷 필터링처리부에서 해당 패킷을 차단할 수 있도록 하고, 보안관리자가 직접 침입차단규칙 및 침입패턴DB를 설정·조회할 수 있도록 하는 것이다.

발명의 구성 및 작용

이를 위해 본 발명은 외부 정보통신망을 통하여 내부망으로 접근하는 모든 패킷 정보에 대하여 침입행위와 관련된 패킷 및 메세지를 탐지하여 차단하는 침입탐지및차단처리부와 침입차단규칙 및 침입패턴DB에 대하여 보안관리자가 직접 설정·조회할 수 있도록 하는 침입차단규칙설정·조회처리부 및 침입패턴DB설정·조회처리부를 제공한다.

침입탐지및차단처리부는 모든 데이터의 패킷정보를 수집하는 패킷수집부, 수집된 모든 패킷을 침입차단규칙에 따라 패킷을 처리하는 패킷필터링처리부, 이를 통과한 모든 패킷에 대하여 침입패턴DB를 참조하여 침입여부를 탐지하고 불법적 침입시도를 탐지할 경우 실시간 자동으로 침입차단규칙에 저장할 수 있는 기능을 수행하는 침입탐지엔진, 침입차단규칙을 저장하는 침입차단규칙저장부, 침입패턴DB를 저장하는 침입패턴DB저장부, 패킷필터링처리부와 침입탐지엔진으로 부터의 로그정보를 처리하는 로그처리부, 침입탐지엔진으로 부터의 경보 및 통보를 처리하는 경보및통보처리부로 구성된다.

이러한 본 발명에 따른 실시간 침입탐지 및 해킹 자동 차단 방법을 첨부된 도면에 의거하여 상세하게 설명하면 다음과 같다.

제1도는 본 발명이 적용되는 인터넷 등 정보통신망과 내부망 사이에 본 발명방법인 실시간 침입탐지 및 해킹 자동 차단에 대한 구성도로, 인터넷 등 정보통신망(1)을 통하여 접근하는 모든 데이터 패킷은 실시간 침입탐지·및 해킹 자동 차단장치(2)를 거쳐 내부망(7)으로 접근하게 되며, 실시간 침입탐지 및 해킹 자동 차단장치(2)내에서는 모든 데이터 패킷에 대해 비정상 행위 여부를 판별 처리하는 침입탐지및차단처리부(3)와 보안관리자(6)가 침입차단규칙 및 침입패턴DB를 설정·조회할 수 있도록 하는 침입차단규칙설정·조회처리부(5) 및 침입패턴DB설정·조회처리부(6)로 구성된다. 침입탐지및차단처리부(3)에서 처리되는 로그 내용과 경보 및 통보 처리 사항에 대해서는 관리서버(8)와 로그서버(9)에 전달할 수 있는 기능을 수행한다.

제2도는 본 발명이 적용되는 실시간 침입탐지 및 해킹 자동 차단 장치(2)에서의 구성요소 및 상호동작도를 나타낸다. 외부 네트워크접속제어부(201)을 통한 모든 데이터 패킷은 패킷수집부(202)에 저장되며, 수집된 데이터 패킷은 패킷필터링처리부(203)에 전달된다. 패킷필터링처리부(203)에서는 침입차단규칙저장부(205)의 규칙에 따라 규칙위반 패킷의 경우 해당 패킷을 폐기 처리하고, 정상 패킷은 로그처리부(211)에 로그정보를 전달한다. 침입탐지엔진(204)은 패킷필터링처리부(203)를 통과한 모든 정상 데이터 패킷을 침입패턴DB저장부(207)의 침입패턴과 비교하여 침입일 경우 침입차단규칙저장부(205)에 해당 규칙을 자동 추가하고 로그처리부(211)와 경보및통보처리부(212)에 침입사실을 전달한다. 침입차단규칙설정·조회부(206)는 침입차단규칙저장부(205)의 침입차단규칙에 대한 설정 및 조회의 기능을 제공하고, 침입패턴DB설정·조회부(208)는 침입패턴에 대한 설정 및 조회의 기능을 제공한다. 관리자콘솔(210)은 콘솔포트(209)를 통해 침입차단규칙설정·조회 및 침입패턴DB설정·조회 작업 환경을 제공한다.

제3도는 본 발명의 전체흐름 개략도로 다음과 같은 단계로 수행된다.

단계 1. 시스템이 시작되어 침입탐지 및 차단 처리이면 단계 1-1로가고 침입패턴DB 설정 조회 처리이면 1-2로 가고 침입차단규칙 설정 조회 처리이면 1-3으로 간다(301).

단계 1-1. 침입탐지 및 차단 처리를 수행한 후 단계 2로 간다(302).

단계 1-2. 침입패턴DB 설정 조회 처리를 수행한 후 단계 2로 간다(303).

단계 1-3. 침입차단규칙 설정 조회 처리를 [redacted]한 후 단계 2로 간다(304).

단계 2. 시스템 종료인지를 판단하여(305) 종료가 아니면 단계 1로 가고, 종료이면 종료한다(306).

제4도는 본 발명의 침입탐지및차단처리부의 실행 및 제어 흐름도로 다음과 같은 단계로 수행된다.

단계 1. 인터넷 등 외부 정보통신망(1)을 통하여 접근하는 데이터 패킷을 패킷수집부(202)로 부터 패킷읽기를 수행한다(401).

단계 2. 종료인지를 판단하여(402) 종료가 아니면 단계 3으로 가고 종료이면 종료한다(403).

단계 3. 단계 1(401)의 수행 결과로 얻어진 결과값인 패킷 정보를 침입차단규칙저장부(205)내의 침입차단규칙(405)과 참조하여 패킷필터링처리를 수행한다(404).

단계 4. 침입인지 판단하여(406) 침입이 아니면 단계 5로 가고 침입이면 패킷폐기를 수행한다(407).

단계 5. 로그처리부(211)에 패킷필터링로그처리를 수행한다(408).

단계 6. 침입탐지엔진(204)이 침입패턴DB저장부(207)내의 침입패턴DB(410)를 참조하여 침입판정을 수행한다(409).

단계 7. 로그처리부(211)에 침입판정결과 로그 처리를 수행한다(411).

단계 8. 침입인지 판단하여(412) 침입이면 단계 9로 가고 침입이 아니면 패킷전송를 수행한다(413).

단계 9. 단계 8(412)의 수행 결과로 패킷이 침입이면 침입탐지엔진(204)은 패킷 정보를 침입차단규칙저장부(205)에 자동 추가하는 침입차단규칙 추가를 수행한다(414).

단계 10. 경보및통보처리부(212)에 경보 및 통보 처리를 수행한다(415).

단계 11. 폐킷폐기를 수행하고 단계 1로 간다(416).

제5도는 본 발명의 침입차단규칙설정·조회부의 실행 및 제어 흐름도로 다음과 같은 단계로 수행된다.

단계 1. 보안관리자(6)가 관리자 콘솔(210)을 통하여 접근권한을 가지고 침입차단 규칙 설정·조회 작업을 시작하면서 조회를 선택하면 단계 5로 가고, 설정을 선택하면 단계 2로 간다(501).

단계 2. 보안관리자(6)가 침입차단규칙 입력을 수행한다(502).

단계 3. 침입차단규칙저장부(205)에 내장된 침입차단규칙(508)에 보안관리자(8)가 침입차단규칙 저장을 수행한다(503).

단계 4. 보안관리자(6)가 종료를 수행한다(504).

단계 5. 침입차단규칙저장부(205)에 내장된 침입차단규칙(508)으로 부터 침입차단규칙읽기를 수행한다(505).

단계 6. 침입차단규칙출력을 수행한다(506).

단계 7. 보안관리자(6)가 종료를 수행한다(507).

제6도는 본 발명의 침입패턴DB설정·조회부의 실행 및 제어 흐름도로 다음과 같은 단계로 수행된다.

단계 1. 보안관리자(6)가 관리자 콘솔(210)을 통하여 접근권한을 가지고 침입패턴 DB 설정·조회 작업을 사작하여 조회를 선택하면 단계 5로 가고, 설정을 선택하면 단계 2로 간다(601).

단계 2. 보안관리자(6)가 침입패턴 입력을 수행한다(602).

단계 3. 침입패턴 DB 저장부(207)에 내장된 침입패턴DB(608)에 보안관리자(6)가 침입패턴 저장을 수행한다(603).

단계 4. 보안관리자(6)가 종료를 수행한다(604).

단계 5. 침입패턴 DB 저장부(205)에 내장된 침입패턴DB(608)로 부터 침입패턴 DB 읽기를 수행한다(605).

단계 6. 침입패턴 DB 출력을 수행한다(606).

단계 7. 보안관리자(6)가 종료를 수행한다(607).

발명의 효과

본 발명은 침입차단시스템의 기능과 침입탐지시스템의 기능을 상호연동시킴으로써, 외부 정보통신망을 통하여 내부 네트워크로 접근하는 모든 침입행위와 관련된 패킷 및 메세지를 탐지하여 실시간 자동으로 차단할 수 있는 기능을 제공한다.

따라서 본 발명은 서비스거부공격(DOS) 등과 같이 외부로 부터의 공격에 취약할 수 밖에 없는 디렉토리 및 웹 서버 등의 내부 시스템에 대하여 안전·신뢰성을 보장할 수 있다.

(57) 청구의 범위

청구항 1.

인터넷 등 외부 정보통신망(1)을 통해 내부망으로의 접근을 시도하는 데이터 패킷에 대하여 감시 및 제어를 수행하는 시스템에 있어서,

외부 네트워크로 부터의 모든 데이터의 접근을 처리하는 외부네트워크접속제어부(201), 모든 데이터 패킷에 대해 비정상 행위 여부를 판별 처리하는 침입탐지및차단처리부(3), 보안관리자(6)가 침입차단규칙을 설정·조회할 수 있도록 하는 침입차단규칙설정·조회처리부(4), 보안관리자(6)가 침입패턴DB를 설정·조회할 수 있도록 하는 침입패턴DB설정·조회처리부(5), 침입탐지및차단처리부(3)내의 침입탐지엔진을 통과한 정상 데이터 패킷을 포함하여 로그처리부(211), 경보및통보처리부(212)의 출력 내용을 내부 네트워크 내의 로그서버(9)와 관리서버(8)로 접근 처리하는 내부 네트워크접속제어부(213), 보안관리자(6)의 침입차단규칙 및 침입탐지DB설정 조회 작업 환경을 제공하는 관리자콘솔(210)을 특징으로 하는 실시간 침입탐지 및 해킹 자동 차단 방법.

청구항 2.

제1항의 침입탐지및차단처리부(3)에 있어서, 모든 데이터의 패킷정보를 수집하는 패킷수집부(202), 수집된 모든 패킷을 침입차단규칙저장부(205)의 침입차단규칙에 따라 처리하는 패킷필터링처리부(203), 패킷필터링처리부(203)를 통과한 정상패킷에 대하여 침입패턴DB저장부(207)의 침입패턴DB를 참조하여 침입여부를 판정하고 불법적 침입시도를 탐지할 경우 실시간 자동으로 침입차단규칙저장부(205)에 해당규칙을 저장할 수 있는 기능을 수행하는 침입탐지엔진(204), 패킷필터링처리부(203) 및 침입탐지엔진(204)의 로그정보를 처리하는 로그처리부(211), 침입탐지엔진(204)의 경보 및 통보를 처리하는 경보 및 통보처리부(212)를 특징으로 하는 실시간 침입탐지 및 해킹 자동 차단 방법.

청구항 3.

제2항의 로그처리부(211)에 있어서, 패킷필터링처리부(203)로 부터 정상 데이터 패킷으로 처리된 패킷필터링로그처리(408)의 정보와 침입판정엔진(204)으로부터 처리된 침입판정결과로그처리(411) 정보를 전달받아 로그서버(9)에 전송하는 구성을 특징으로 하는 실시간 침입탐지 및 해킹 자동 차단 방법.

청구항 4.

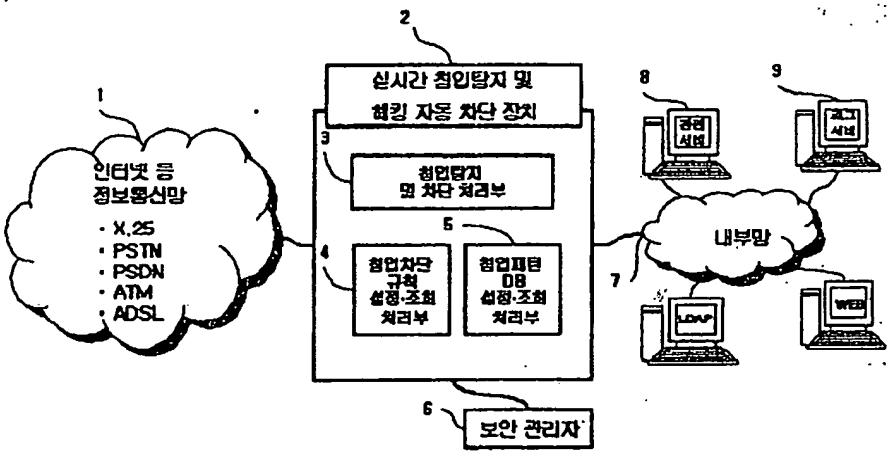
제1항의 침입차단규칙설정·조회처리부(4)와 침입패턴 DB설정·조회처리부(5)에 있어서, 보안관리자(6)가 침입차단규칙저장부(205)에 내장된 침입차단규칙을 조회, 입력 및 저장할 수 있고, 침입패턴DB저장부(207)에 내장된 침입패턴DB(608)를 조회, 입력 및 저장할 수 있도록 환경을 제공하는 콘솔포트(209) 및 관리자콘솔(210)을 특징으로 하는 실시간 침입탐지 및 해킹 자동 차단 장치 방법.

청구항 5.

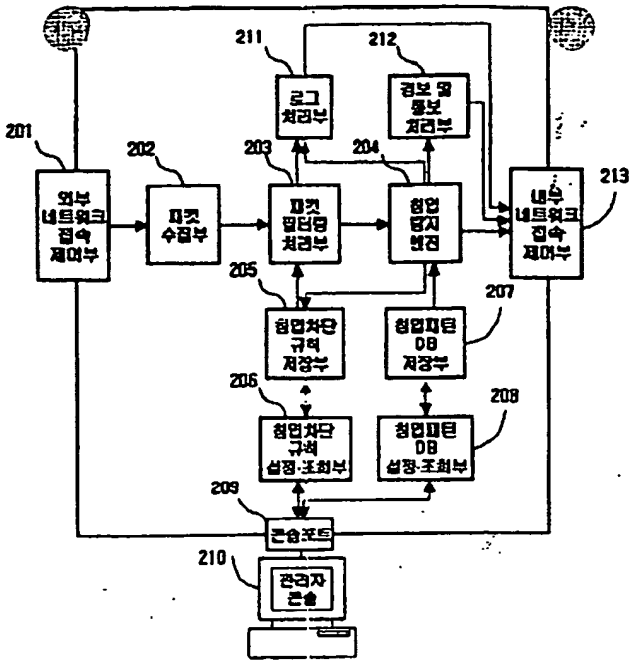
상기 제1항, 제2항, 제3항, 제4항이 실현되기 위한 제어 및 실행 흐름도(제4도, 제5도, 제6도)

도면

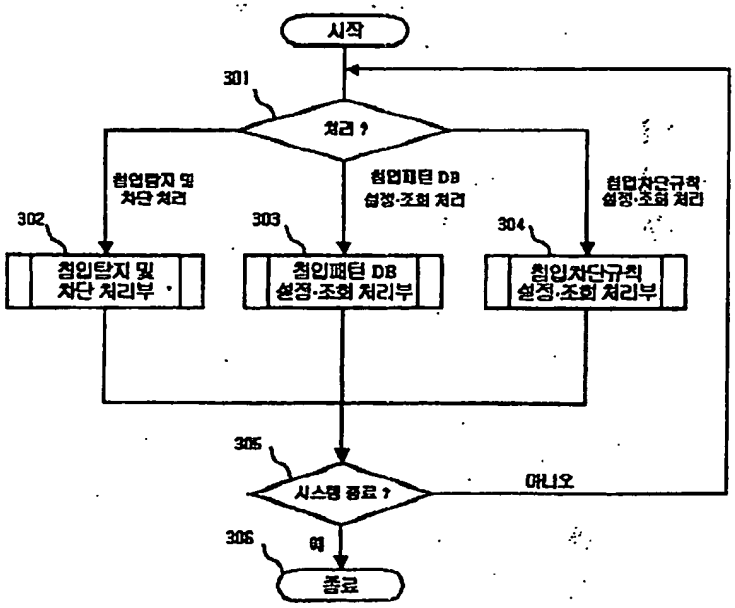
도면 1



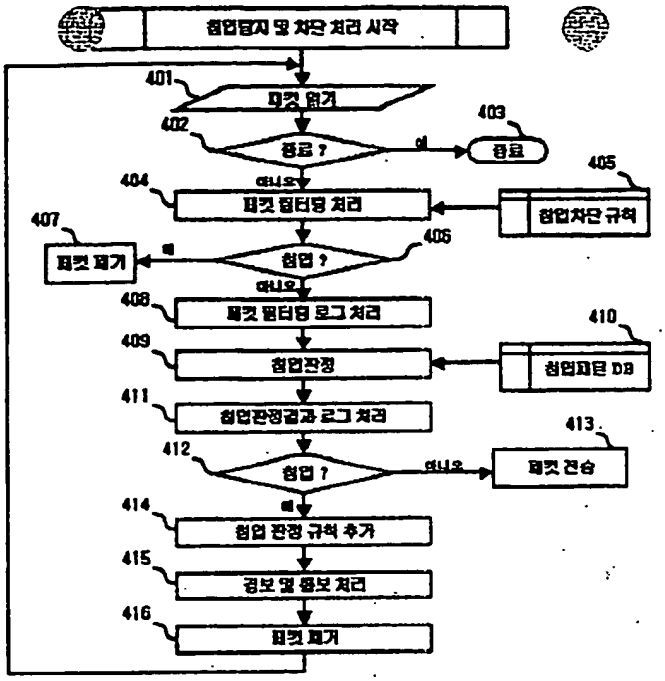
도면 2


211
212
로그 처리부
경보 및 통보 처리부
201
202
203
204
213
외부 네트워크 접속 제어부
패킷 수집부
패킷 필터링 처리부
침입 탐지 엔진
내부 네트워크 접속 제어부
205
207
침입차단 규칙 저장부
침입패턴 DB 저장부
206
208
침입차단 규칙 설정·조회부
침입패턴 DB 설정·조회부
209
콘솔포트
210
관리자 콘솔

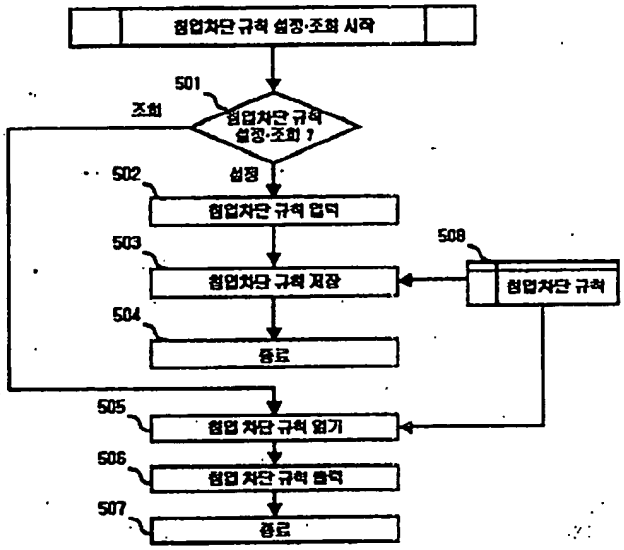
도면 3


시작
301
처리 ?
침입탐지 및 차단 처리
침입패턴 DB 설정·조회 처리
침입차단규칙 설정·조회 처리
302
303
304
침입탐지 및 차단 처리부
침입패턴 DB 설정·조회 처리부
침입차단규칙 설정·조회 처리부
305
시스템 종료 ?
아니오
306
예
종료

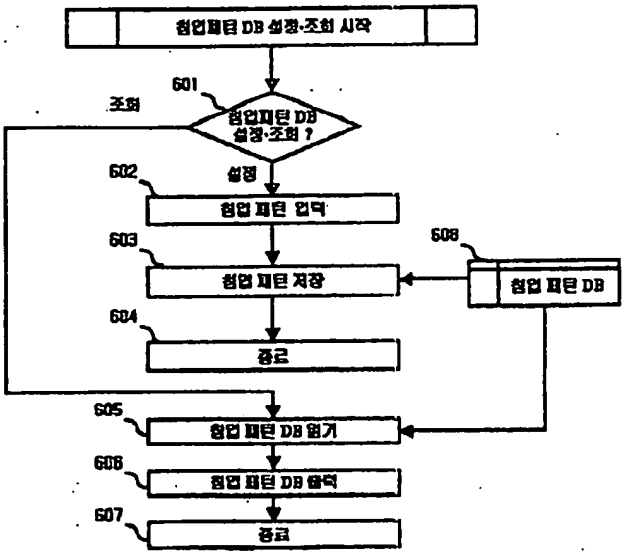
도면 4


침입탐지 및 차단 처리 시작
401
패킷 읽기
402
종료 ?
예
403
종료
아니오
404
패킷 필터링 처리
405
침입차단 규칙
407
패킷 폐기
예
406
침입 ?
아니오
408
패킷 필터링 로그 처리
409
침입판정
410
침입패턴 DB
411
침입판정결과 로그 처리
412
침입 ?
아니오
413
패킷 전송
예
414
침입 판정 규칙 추가
415
경보 및 통보 처리
416
패킷 폐기

도면 5


침입차단 규칙 설정·조회 시작
501
조회
침입차단 규칙 설정·조회 ?
설정
502
침입차단 규칙 입력
503
침입차단 규칙 저장
508
침입차단 규칙
504
종료
505
침입 차단 규칙 읽기
506
침입 차단 규칙 출력
507
종료

도면 6


침입패턴 DB 설정·조회 시작
601
조회
침입패턴 DB 설정·조회 ?
설정
602
침입 패턴 입력
603
침입 패턴 저장
608
침입 패턴 DB
604
종료
605
침입 패턴 DB 읽기
606
침입 패턴 DB 출력
607
종료